PCT / IB 04 / 00854
16 MAR 2004

INVESTOR IN PEOPLE

BEST AVAILABLE COPY

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

REC'D 26 MAR 2004
WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 17 December 2003

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

27MAR03 E795603-1 D02879
P01/7700 0.00-0307033.1

Patents Form 1/77

Patents Act 1977
(Rule 16)

THE PATENT OFFICE
B
27 MAR 2003
NEWPORT

The Patent Office

1/77

Request for grant of a patent
(See notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP10 8QQ

1. Your reference — PHGB 030028GBP

2. Patent application number
(The Patent Office will fill in this part) — 0307033.1 — 27 MAR 2003

3. Full name, address and postcode of the or of each applicant (*underline all surnames*)

KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN
THE NETHERLANDS

Patents ADP Number (*if you know it*) — 07419294001

If the applicant is a corporate body, give the country/state of its incorporation — THE NETHERLANDS

4. Title of the invention — METHOD OF PROTECTING A RADIO ENVIRONMENT

5. Name of your agent (*if you have one*)

"Address for service" in the United Kingdom to which all correspondence should be sent (*including the postcode*)

Philips Intellectual Property & Standards
Cross Oak Lane
Redhill
Surrey RH1 5HA

Patents ADP number (*if you know it*) — 08359655001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (*if you know it*) the or each application number

Country	Priority Application number	Date of filing

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing (*day/month/year*)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (*Answer "Yes" if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

Enter the number of sheets for any of the following items you are filing with this form.
Do not count copies of the same document.

Continuation sheets of this form	
Description	12
Claims(s)	3
Abstract	1
Drawings	6

18

10. If you are also filing any of the following, state how many against each item:

Priority Documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (*Patents Form 7/77*)

Request for preliminary examination and search (*Patents Form 9/77*)

Request for substantive examination (*Patents Form 10/77*)

Any other documents (*Please specify*)

11. I/We request the grant of a patent on the basis of this application.

Signature A G WHITE

Date 26/3/2003

12. Name and daytime telephone number of person to contact in the United Kingdom 01293 81 5576 P J MABEY

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered "Yes" Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

DESCRIPTION

METHOD OF PROTECTING A RADIO ENVIRONMENT

The present invention relates to a method of protecting a radio environment, particularly inhibiting the operation of and/or preventing the establishment of wireless networks, in restricted geographical areas such as hospital departments using sensitive electronic equipment which could be affected adversely by unauthorised electromagnetic radiation or in a subsisting wireless network.

Blocking of radio transmissions is not in itself new, for example, radio jamming by governmental agencies of undesired foreign broadcast transmissions not only in war time but also in peacetime. Such jamming involves making transmissions of say noise on the same frequency as the unwanted broadcast transmissions. In the field of cellular telephones it is known for example in GSM systems for people to illegally jam transmissions by transmitting wideband noise. A significant drawback to these known methods of radio jamming is that it is non-selective in that all transmissions are affected.

However there are situations in which a multitude of users are sharing a band of frequencies, such as the ISM band (2.400 to 2.4835 GHz), and attempts to jam one user affects many other users. Many authorised wireless networks, such as those operating in accordance with evolving standards such as Bluetooth™, Zigbee and IEEE 802.11b, may operate in a restricted geographical area such as a hospital or laboratory site but within that area there may be localities where unauthorised establishment of a wireless network should be prevented. However the method of prevention should avoid interfering with the operation of authorised wireless networks. The simple transmission of wideband noise would not achieve such a condition.

US Patent Specification 6,377,608 discloses protecting a wireless local area network (WLAN) operating in the ISM band by means of a wireless

beacon operating in the vicinity of an access point of the WLAN. The beacon transmits in a part of the ISM band which does not overlap that used by the WLAN. Ad hoc radios, such as frequency hopped spread spectrum radios, belonging to other networks operating in the same ISM band have beacon responsive radio control mechanisms which monitor the beacon channel for the presence of the wireless beacon. If detected, in one mode the ad hoc radio is adjusted so that it transmits in a selected portion of the ISM band other than that used by the WLAN. Other interference avoidance modes include deferring transmission on selected channels, altering frequency hopping pattern, changing from a frequency hopping mode to a fixed frequency mode, deactivating the transmitter of the ad hoc radio and reducing the transmit power of the ad hoc radio. The wireless beacon may be pulsed in order to reduce the overall transmit power. The ad hoc radio may monitor for the presence of a beacon signal by periodically switching its frequency synthesiser to the beacon frequency or frequencies.

The use of beacon signals contributes undesirably to the transmissions in the ISM band which themselves may interfere with other users of the ISM band as well as affect equipment which requires to be in an environment free from spurious electromagnetic radiation. Also it is the responsibility of the ad hoc radio to take action to avoid interfering with the WLAN which has the drawback that it may fail to respond to beacon signals because it cannot receive them and/or it is non-compliant due to a defect or the user is able to override any action instituted by the ad hoc radio.

An object of the present invention is for a system to be protected to take whatever action is appropriate to prevent an interferer from interfering with its operation.

According to one aspect of the present invention there is provided a method of protecting a radio frequency environment, comprising detecting the presence of an interfering terminal involved with a radio transmission in an environment to be protected, determining at least one characteristic of the radio transmission, and using knowledge of the at least one characteristic to

render ineffective radio transmissions by the interfering terminal in the environment to be protected.

According to a second aspect of the present invention there is provided a wireless network comprising a plurality of radio stations, at least one of said radio stations functioning as a policing terminal to protect the service area of the network against signals produced by an interfering terminal, the policing terminal having means for determining at least one characteristic in signals produced by the interfering terminal and for using knowledge of the at least one characteristic to render ineffective signals produced by the interfering terminal.

According to a third aspect of the present invention there is provided a policing terminal for protecting a radio frequency environment against signals produced by an interfering terminal, the policing terminal having means for determining at least one characteristic in signals produced by the interfering terminal and for using knowledge of the at least one characteristic to render ineffective signals produced by the interfering terminal.

Implementing the method in accordance with the present invention does not conflict with the current FCC rules for transmission in the ISM band and moreover causes minimum of disturbance to other systems operating in the ISM band. More particularly the method in accordance with the present invention enables the operation of unauthorised wireless network devices in a geographical area to be controlled whilst permitting operation of authorised wireless network devices in the same frequency band. The method in accordance with the present invention may be reactive in that a response is generated once an interfering terminal has been detected or pro-active in that the policing terminal actively looks out for an interfering terminal so that it can take action before the interfering terminal becomes a nuisance.

The present invention will now be described, by way of example, with reference to the accompanying drawings, wherein:

Figure 1 is a block schematic diagram illustrating a service area of a wireless network,

Figure 2 is a block schematic diagram illustrating a geographical environment in which is located sensitive apparatus to be protected from electro-magnetic radiation,

Figure 3 is a block schematic diagram of a policing terminal which can be used to disable interfering radio entering a service area of a wireless network or a protected geographical environment,

Figures 4 and 5 together comprise a flow chart illustrating methods of protecting an environment when a wireless network is present,

Figure 6 is a flow chart illustrating a transmit method of protecting an environment when a low power LAN does not exist,

Figure 7 is a flow chart illustrating a receive method of protecting an environment when a wireless network does not exist, and

Figure 8 is a flow chart illustrating other receive methods of protecting an environment when a wireless network does not exist.

In the drawings the same reference numerals have been used to indicate corresponding features.

For convenience of description the present invention will be described with reference to interfering radio devices operating in accordance with the Bluetooth™ standard but it is to be understood that the teachings of the present invention can be applied to wireless local area networks (WLANS) using radio devices operating in accordance with other standards such as Zigbee and IEEE 802.11b which also operate in the ISM band, namely 2.4000 to 2.4835 GHz. Transmissions may be direct sequence spread spectrum (DSSS) or frequency hopped spread spectrum (FHSS).

Details of the Bluetooth™ Specification Version 1.1 are publicly available and are incorporated by way of reference. However certain details of the Specification relevant to the implementation of the present invention will be given.

The Bluetooth™ radio frequency system is a frequency hopping spread spectrum system where data packets having a duration of 625μs are transmitted in defined channel frequencies lying in the ISM band, the individual

channels being separated by 1MHz. The hopping sequence is determined by the master station.

Every Bluetooth™ terminal has an internal system clock which determines the timing and hopping of a transceiver in the terminal. For synchronisation with other terminals forming the wireless network, the current master station notifies its slave stations of what timing offsets each should apply to its own clock in order to mutually synchronise the local clocks in the terminals. The master station always has full control over the wireless network Also due to a stringent time division duplex (TDD) scheme slave stations can only communicate with the master station and not to other slave stations.

It is possible for a master-slave switch to take place where there is a role change in which the master slave becomes a slave station and the former slave station becomes the master station. However the wireless network parameters which were derived from the address and clock of the original master station remain unchanged.

A data packet has several fields including synchronisation, preamble and address, a header with link information and user data.

Referring to Figure 1, there is shown a closed service area PSA of a wireless network in which authorised radio terminals 10, 12, 14 are either fixed or able to roam and maintain radio contact with each other. The terminals 10, 12 and 14 operate in accordance with the IEEE 802.11b standard. One of the terminals, say the terminal 10 functions as a master station MS and the remainder of the terminals 12, 14 function as slave stations.

The wireless network is a closed network insofar that other interfering terminals, such as terminal 16, entering the service area PSA will not only be prevented from joining the wireless network but also will actively be dissuaded from operating. The master station 10 can assume the role of policing the wireless network or a dedicated policing terminal PT can monitor the radio activity and in response to detecting the presence of an interfering terminal can take action to deter it. Ideally in this role the policing terminal PT is able to adopt the operating mode, for example Bluetooth™, in order to be able to

communicate with the interfering network to which the terminal 16 belongs as well as its own IEEE 802.11b network.

Referring to Figure 2, the situation illustrated relates to protecting a piece of apparatus 18 whose operation is adversely affected by electromagnetic radiation such as that emitted by a Bluetooth™ terminal in an excluded geographical area 20 around the apparatus 18. The protection is effected by a policing terminal PT monitoring for unwanted radio activity in the geographical area 20.

Figure 3 is a block schematic diagram of a policing terminal PT the architecture of which is similar to the terminals 10, 12, 14 and perhaps 16. The policing terminal comprises an antenna 22 which is connected to a receiver 24 and a transmitter 26. A processor 28 is provided for controlling the operation of the terminal in accordance with a program stored in a memory M1. The processor 28 has a plurality of ports for connection to the receiver 24, the transmitter 26, a LCD driver 30 for driving a LCD panel 32, a frequency synthesiser 34, a noise generator 36, a memory M2 for storing the operating standard, for example IEEE 802.11b, of the wireless network that it is to be protected and a memory M3 for storing the operating standard, for example Bluetooth™ (abbreviated as BT), of the interfering terminal 16.

The policing terminal PT can respond to the detection of unwanted electromagnetic radiation in the ISM band, in this instance interfering Bluetooth™ signals in several ways depending on particular circumstances.

A normal BT packet contains a short sync word, a preamble containing the BT address of the destination (or slave) terminal, a header that contains other link information and finally the actual user data. The data and header are normally mixed up with a random signal that is generated by reference to the master station's clock (6 of its bits) to ensure that the signal transmitted over the air is sufficiently random in nature to allow the radio hardware to function correctly. A BT network hops from one frequency to another on each packet, the pattern or the hopping sequence is derived from the clock in the master station.

A normal BT connection set-up works as follows: A master station transmits a plurality of inquiry packets on several frequencies. These inquiry packets have a general address in its preamble so it is easy to search for. In order for a terminal to be contacted it must be looking for these inquiry packets. There is no requirement that any terminal should be doing this at any particular time, if ever. The normal enquiry procedure can take up to 40 seconds, although it is usually completed quicker, due to the random frequencies and timing of the two terminals' transmissions and receptions.

The inquiry response from the slave station is a conventional FHS packet which contains the slave station's address and clock. This allows the master station to address directly the slave station when the link is set up properly during the page function. The page function is carried out once the master and slave stations know of each other's existence. The master station sends a paging packet to the specific slave station with the slave station's address in the packet preamble. The response to the page by the slave station is just an acknowledgement of receipt. The master station then responds with another FHS packet to give the slave station the clock timing so that the final link hopping sequence can be used. The next communication between the two stations is the data.

The terminal that starts the process will normally become the master station of the network, although as mentioned above a master-slave switch can be made when the link is established.

In order to implement the method in accordance with the present invention there are two categories of methods to prevent BT networks from existing, namely, (1) removing an already existing network, and (2) preventing the establishment of a network when none exists already.

Figures 4 and 5 comprise a flow chart of the type of operations involved when implementing category (1). Referring to Figure 4, block 22 relates to a policing terminal PT detecting that an existing wireless network interferes with the protected wireless network. Block 24 relates to the policing terminal PT adapting itself to mimic a Bluetooth™ slave station and endeavouring to join the interfering wireless network by transmitting a normal inquiry response to

inquiry messages transmitted by the master station of the interfering wireless network. Block 26 relates to checking if the attempt has been successful. If the response is Yes (Y) then in block 28 the master station allows the slave station to join the interfering wireless network. In block 30 the slave station attempts to swap the master/slave roles. In a block 32 a check is made that the master-slave swap has been successful. In the course of the successful swap the slave station as the new master station will be given the addresses of other slave stations in the interfering wireless network. If the swap has been successful (Y) then in block 34 the new master station can transmit a disconnect message to each of the slave stations. A user may try to rejoin the wireless network only to find that his slave station disconnects. It is assumed that if frustrated enough times the user will give up. Thus the interfering wireless network is closed.

Thereafter the policing terminal PT checks that the disconnection of the slave station has been successful, block 37. If it has been successful (Y) then the policing terminal PT can either continue mimicking the master station, block 38, or try to restart the original (interfering) master station, block 39. In block 40 a check is made to see if the original master station has restarted. If the answer is yes (Y) then in block 41 the original master station is disconnected. If the answer in the block 40 is negative (N) then the flow chart reverts to the block 39. The output from the block 41 also reverts to the block 39.

If the answer in the block 37 is negative (N) the flow chart reverts to the block 34.

In an optional variant variant of this flow chart, block 36 relates to an audible message or a message to be displayed on the LCD panel being sent to the slave stations saying that the network is being terminated and giving a reason for the termination thus hopefully avoiding a user trying to re-join the network. Thereafter the flow chart proceeds to the process stage 34.

Reverting to the block 32, in the event of a failure (N) in the attempt to swap master and slave roles, the policing terminal PT is nevertheless a member of the interfering wireless network and as such is given details of the

hopping sequence. In a block 42 the policing terminal PT listens to all the packet headers in order to learn the BT addresses of all the terminals in the wireless network. In a block 43 the policing terminal PT mimics the master station. In block 44 a check is made to see if the mimicry has been successful. If it is successful (Y) then in block 45 the policing terminal PT tells all the other slave stations to disconnect. If this is unsuccessful (N), in block 46 the policing terminal PT transmits a short burst of noise onto the current frequency during preamble or sync word to effectively and efficiently destroy each packet on the interfering network. However depending on the operating standard of the protected wireless network there is a risk of it being affected adversely if there is coincidence with one or more of the frequencies of its hopping sequence and clocks. In which case the policing terminal PT may decide to do nothing, block 47, thereby avoiding interfering with the wireless network it is protecting.

Reverting to the block 26, if the policing terminal PT is refused access to the interfering network (N) the master station's clock is unknown. Referring now to Figure 5, in block 48 the policing terminal PT listens to the wireless network and in block 50 it calculates the slot timing of the interfering network. Additionally in block 52 the policing terminal PT listens to the BT addresses of all the devices in the interfering network, this being possible as the normal BT packet header gives the address of the receiving (or slave) station. In block 54 a check is made that all the addresses have been obtained. If the answer is Yes (Y) then in block 56 the policing terminal PT mimics a BT master station and transmits a disconnect signal to each of the stations in the interfering wireless network on a single frequency with a random whitening pattern. This equates to being correct once in every 3 seconds (625μs x 79 x 64). In the event of not having obtained all the addresses (N) (block 54) the flow chart reverts to the block 52.

Block 58 relates to the policing terminal PT, gaining, for example by a method to be described later, the address of the master station and clock of the interfering network. In block 60 the policing terminal PT calculates the hopping pattern of the interfering wireless network. In block 62 the policing

terminal PT having determined the hopping pattern disables the interfering wireless network more rapidly than would have been possible otherwise.

Blocks 64 to 68 relate to another technique which can be used when access is denied by a master station to its wireless network. In the block 64 the policing terminal PT scans the entire ISM band in less time than the duration of one BT packet for the detection of signals. Block 66 relates to checking if any signals have been detected. If they have (Y) then in block 68 noise is transmitted on top of the signals. If no signals are detected (N) in the block 66 the flow chart reverts to the input of the block 64. As a practical point in view of the time to retune a frequency synthesiser it may be necessary to split the ISM band into larger portions. As long as the noise transmissions from the policing terminal PT catch the end of each BT packet the link is destroyed in practical terms and the user or application (in the case of fixed equipment) will give up.

In all the applications in which the policing terminal PT is trying to mimic another device it is preferable for it to start its transmissions very slightly earlier, say 10μs earlier in the case of Bluetooth™ than that of the station which it is trying to imitate. By doing this the receiving station is more likely to lock onto the transmissions from the policing terminal PT than those of the station to be disconnected.

Figures 6, 7 and 8 are flow charts relating to the second category of preventing the establishment of a network when none exists already or a network has been disconnected. This category can be divided into transmit (Figure 6) and receive (Figures 7 and 8) sub-categories.

In the case of transmit sub-category (Figure 6), if it is desired to protect a IEEE 802.11b network, in block 70 a policing terminal PT transmits inquiry packets synchronised not to disrupt the protected network's transmissions. This will gather up any new stations roaming into the range of the protected network. In block 71 the policing terminal PT connects to those stations which respond to the inquiry packets. In block 72 the policing terminal PT captures their clock and address and in block 73 stores this information so that if in future they try to initiate any networks themselves, their clock and BT address will be generally known and from this information it will be possible to derive its

hop pattern later. Finally in block 74 the slave stations gathered-up are either disconnected or kept in a low power mode.

In a first receive sub-category (Figure 7), block 75 relates to the policing terminal PT listening for different types of packets which may occur when a new WLAN is forming. In block 76 a check is made to see if any packets have been detected. If the answer is yes (Y) then in block 77, the policing terminal PT mimics the master station and proceeds to disconnect its slave stations. Alternatively in block 78 the policing terminal PT interferes with the soon-to-be created master station.

In the receive sub-category (Figure 8), in block 80 the policing terminal PT listens for a new device transmitting inquiry packets. In block 82 the policing terminal PT detects such packets. At this point various options may be followed. Firstly in block 84 the policing terminal PT can transmit wideband noise with a view to disrupt the formation of a network. The wider the bandwidth the policing station PT can detect and transmit noise over the better.

Secondly in block 86, the policing terminal PT mimics the operating standard of the interfering wireless network and responds to the inquiry packet by attempting to join the new network as a slave station. In block 88 the slave station attempts to effect a master/slave swap. In block 90 a check is made to see if the attempt is successful and if it is (Y) the new master endeavours to disconnect the other slave stations (block 94). Optionally in block 96 the policing terminal PT transmits audible or data messages to the slave stations informing them of the impending termination. If the master/slave swap in unsuccessful (N) the flow chart follows the process steps 108 to 118 to be described later.

Thirdly, if while the policing terminal PT is listening it hears other network setup packets there are actions which can be taken at each stage. If an inquiry packet is heard from a device then in block 98 the inquiry packet is duplicated and in block 100 the policing terminal PT uses the duplicate inquiries to snare any potential slave station and thus keep it from other

stations. Alternatively in block 102 the policing terminal PT may try to disrupt the inquiry packets with noise.

Fourthly, in a further alternative the policing terminal PT in block 104 mimics a slave station and in block 106 convinces the master station to stop looking for his real slave.

Fifthly, in block 108 the policing terminal PT listens for a paging packet. If the master station's response is heard during a paging period, then in block 110 the policing terminal PT detects the master's clock. In block 112 the policing terminal PT attempts to mimic the master station. In block 114 a check is made to see if the attempt has been successful, if it has (Y) then in block 116 the other slave stations are told to disconnect. Alternatively if the attempt has been unsuccessful (N) then in block 118 the policing terminal PT transmits noise.

In the present specification and claims the word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. Further, the word "comprising" does not exclude the presence of other elements or steps than those listed.

From reading the present disclosure, other modifications will be apparent to persons skilled in the art. Such modifications may involve other features which are already known in the design, manufacture and use of low power local area networks and component parts therefor and which may be used instead of or in addition to features already described herein. Although claims have been formulated in this application to particular combinations of features, it should be understood that the scope of the disclosure of the present application also includes any novel feature or any novel combination of features disclosed herein either explicitly or implicitly or any generalisation thereof, whether or not it relates to the same invention as presently claimed in any claim and whether or not it mitigates any or all of the same technical problems as does the present invention. The applicants hereby give notice that new claims may be formulated to such features and/or combinations of such features during the prosecution of the present application or of any further application derived therefrom.

CLAIMS

1. A method of protecting a radio frequency environment, comprising detecting the presence of an interfering terminal (16) involved with a radio transmission in an environment (PSA or 20) to be protected, determining at least one characteristic of the radio transmission, and using knowledge of the at least one characteristic to render ineffective radio transmissions by the interfering terminal in the environment to be protected.

2. A method as claimed in claim 1, characterised in that the radio frequency environment includes a policing terminal (PT) for protecting the environment.

3. A method as claimed in claim 2, characterised in that the policing terminal is able to operate in the mode of the interfering terminal.

4. A method as claimed in claim 2, wherein the radio frequency environment comprises a wireless network to be protected, characterised in that the policing terminal is a member of wireless network to be protected and in that the policing terminal is able to operate in the mode of the network to be protected as well as the mode an interfering network of which the interfering terminal is a member.

5. A method as claimed in claim 4, characterised by the policing terminal joining the interfering wireless network as a slave station, by the policing terminal becoming the master station of the interfering wireless network, and by the policing terminal transmitting instructions to other slave stations of the interfering network to close down.

6. A method as claimed in claim 4, wherein the interfering terminal is a member of an interfering wireless network, characterised in that the at least one characteristic is a frequency hopping sequence, in that the policing

terminal joins the interfering wireless network as a slave station, in that the policing terminal uses knowledge of the hopping sequence to determine addresses of other slave stations in the interfering wireless network and in that the policing terminal transmits disconnect signals to slave stations of the interfering network.

7. A method as claimed in claim 4, characterised by the policing terminal listening to the RF band of interest and determining the slot timing and the addresses of all the stations on the interfering network and by the policing terminal transmitting a disconnect signal to each station on a single frequency with random data whitening pattern

8. A method as claimed in claim 4, characterised by the policing terminal scanning the entire RF band of interest and, in response to detecting a signal, by transmitting noise on top of it.

9. A method as claimed in any one of claims 5 to 8, characterised by the policing terminal commencing its transmissions to an interfering slave station just prior to transmissions to the same slave station by a master station of the interfering wireless network.

10. A wireless network comprising a plurality of radio stations (10, 12, 14, PT), at least one of said radio stations functioning as a policing terminal (PT) to protect the service area of the network against signals produced by an interfering terminal (16), the policing terminal having means (28) for determining at least one characteristic in signals produced by the interfering terminal and for using knowledge of the at least one characteristic to render ineffective signals produced by the interfering terminal.

11. A policing terminal for protecting a radio frequency environment against signals produced by an interfering terminal (16), the policing terminal having means (28) for determining at least one characteristic in signals

produced by the interfering terminal and for using knowledge of the at least one characteristic to render ineffective signals produced by the interfering terminal.

12. A policing terminal as claimed in claim 11, wherein the radio frequency environment comprises a wireless network to be protected, characterised in that the policing terminal is a member of a wireless network to be protected and in that the policing terminal is able to operate in the mode of the network to be protected as well as the mode an interfering network of which the interfering terminal is a member.

13. A method of protecting a radio frequency environment, substantially as hereinbefore described with reference to the accompanying drawings.

14. A wireless network constructed and arranged to operate substantially as hereinbefore described with reference to and as shown in the accompanying drawings.

15. A policing terminal constructed and arranged to operate substantially as hereinbefore described with reference to and as shown in the accompanying drawings.

ABSTRACT

METHOD OF PROTECTING A RADIO ENVIRONMENT

A method of protecting a radio frequency environment, such as a low power wireless LAN (PSA) or a radio free environment (20), comprises a policing terminal (PT) detecting the presence of an interfering terminal (16) in the protected environment and actively rendering ineffective or terminating transmissions by the interfering terminal. Various options can be followed by the policing terminal (PT) including (a) attempting to become the master station of a network of which the interfering terminal is a member and instructing the members to close down or (b) failing to become the master station and transmitting interference signals for at least a selected portion, for example preamble and sync, of the duration of a data packet transmitted by the interfering station.

(Figure 1)

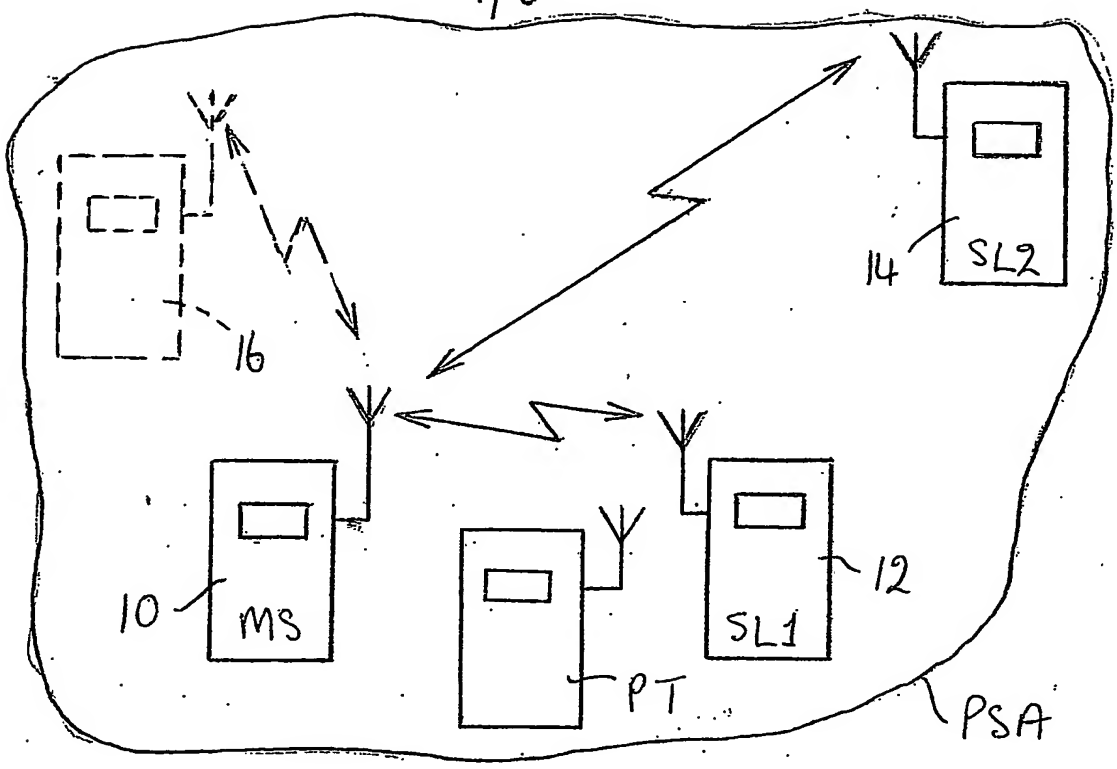

Fig. 1

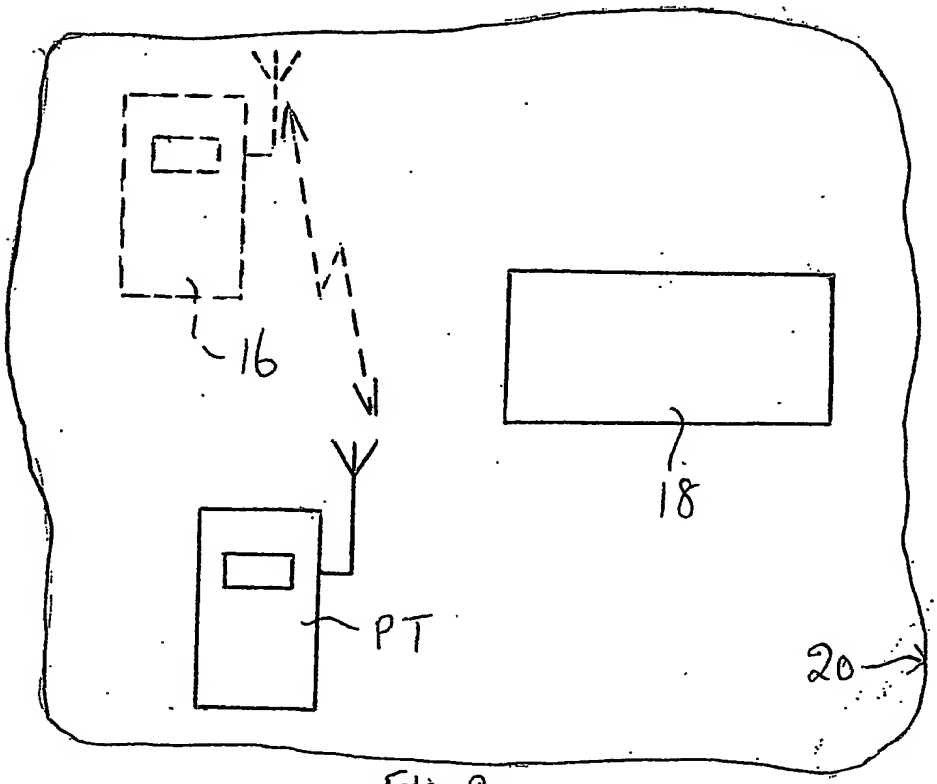

Fig. 2

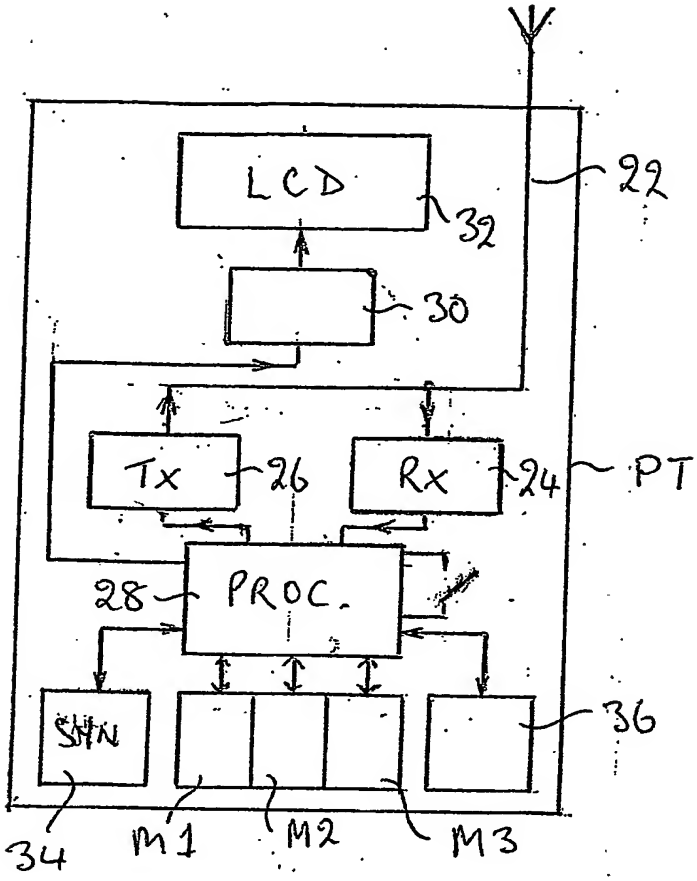

Fig. 3

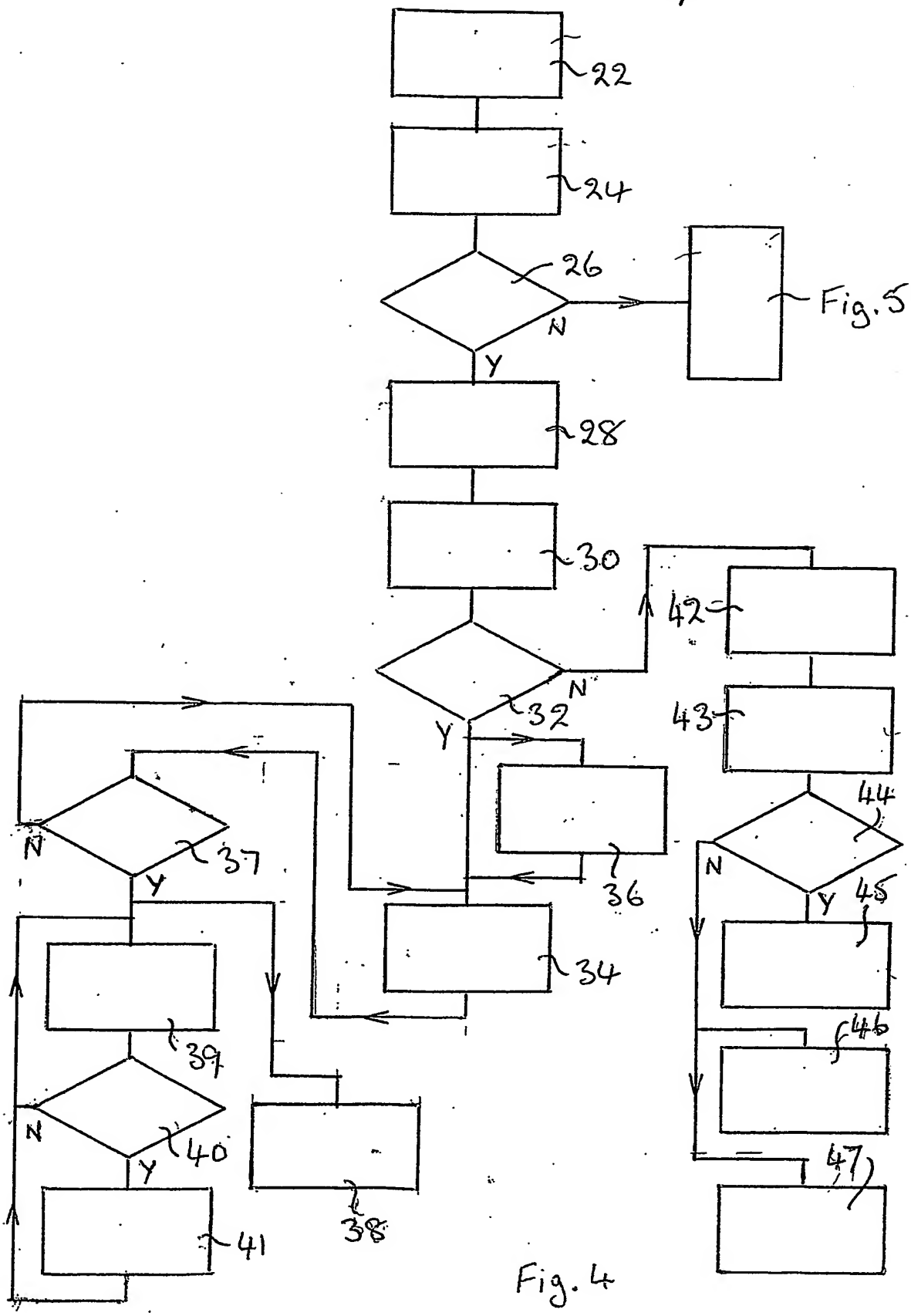
22
24
26
N
Y
Fig.5
28
30
42
32
N
Y
43
44
N
Y
45
46
47
36
34
37
N
Y
39
40
N
Y
41
38

Fig. 4

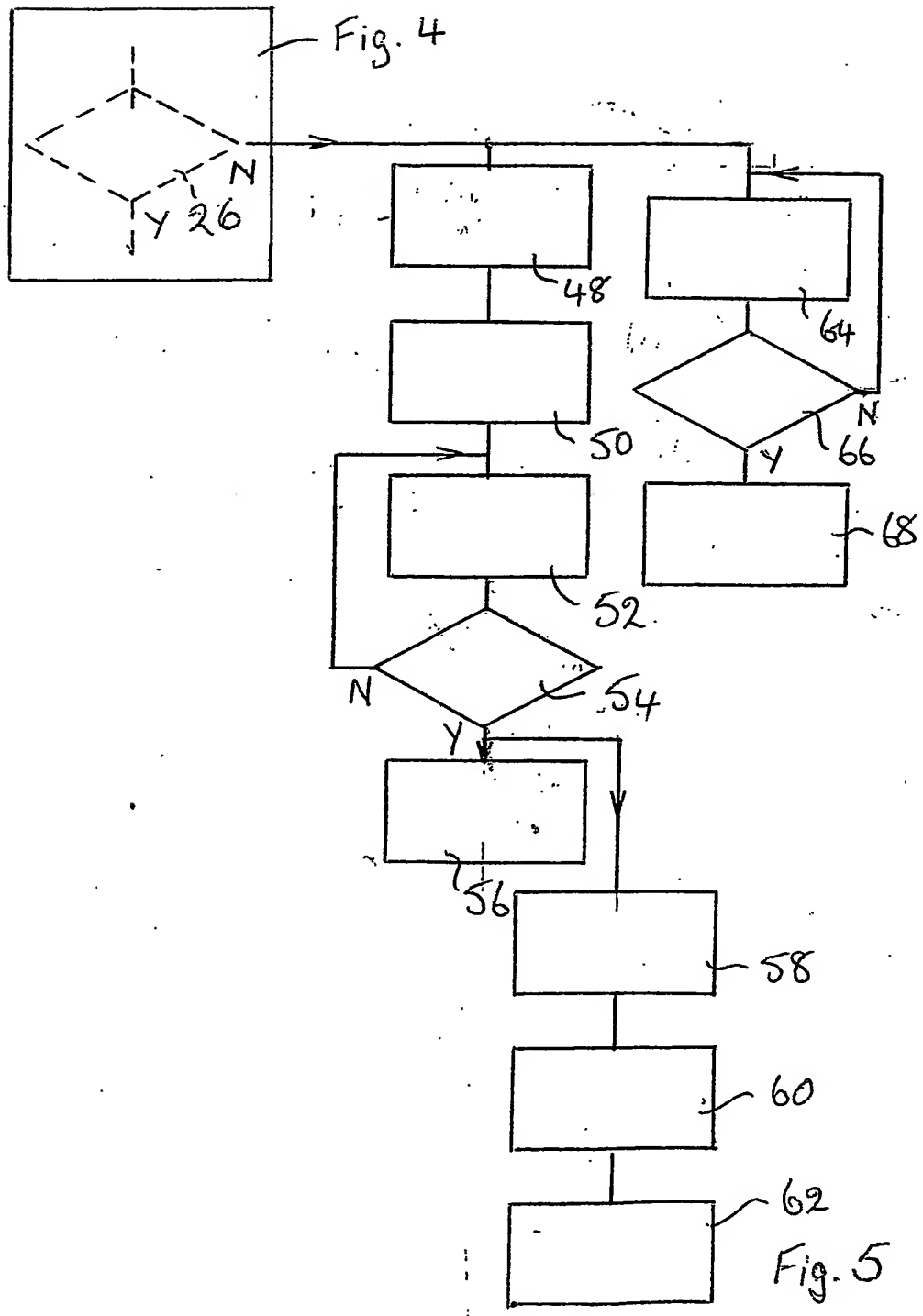

Fig. 4

Fig. 5

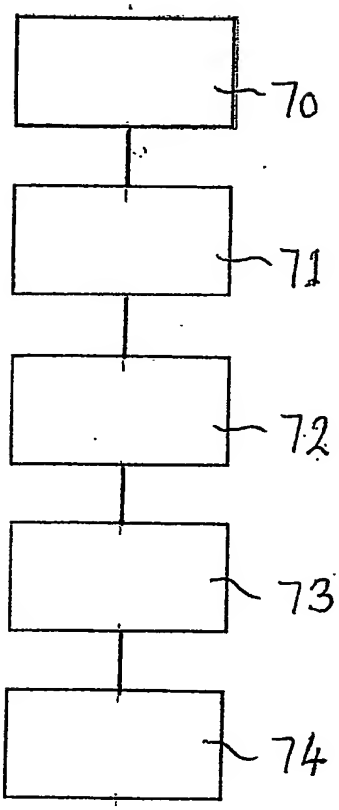

Fig. 6

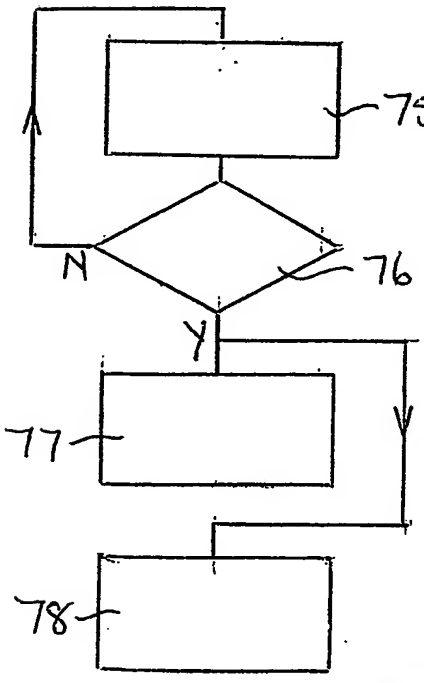

Fig. 7

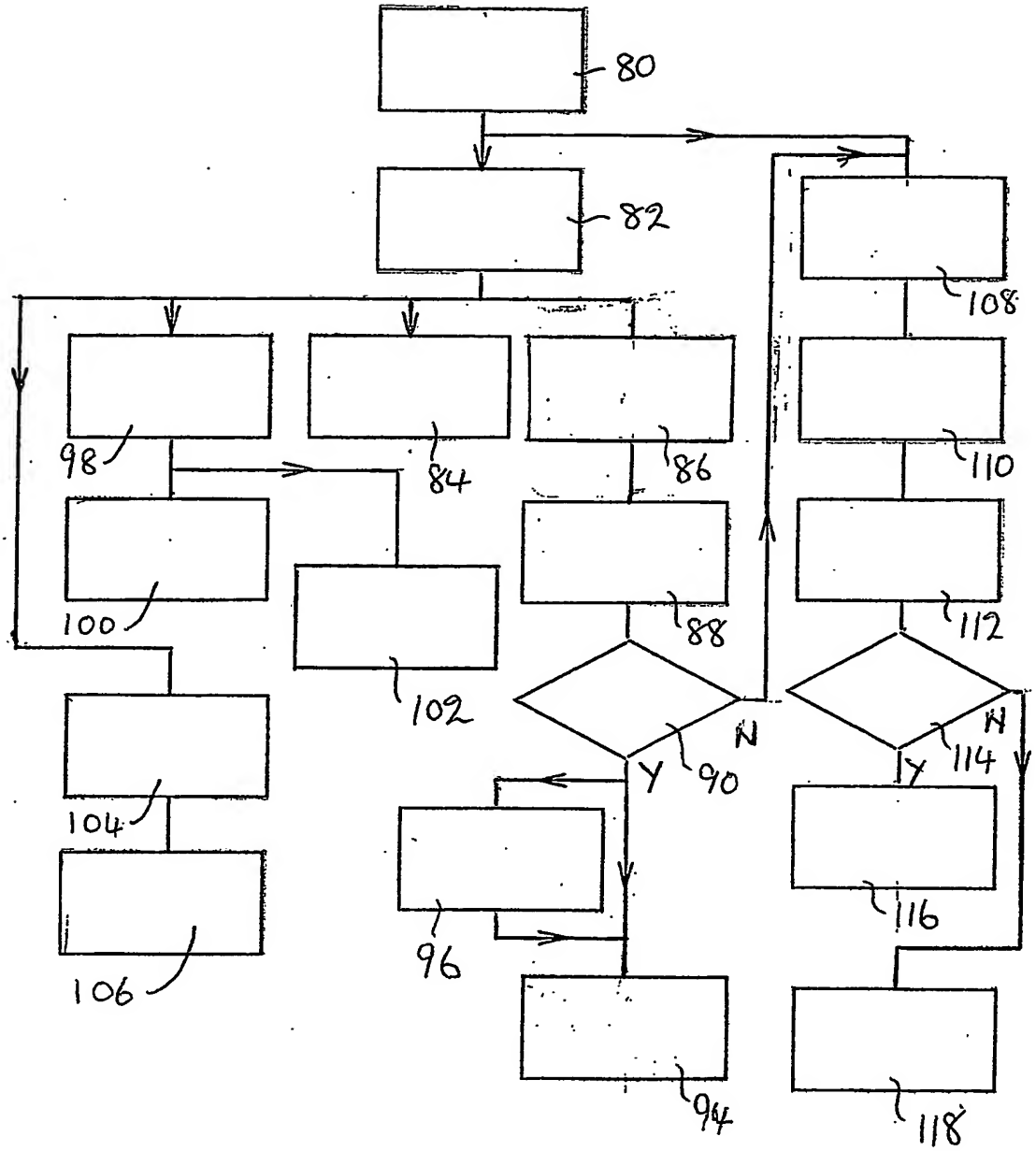
80
82
108
98
84
86
110
100
88
112
102
N
N
Y
90
Y
114
104
116
96
106
94
118

Fig. 8

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.